CHAPTER

# 15

# SECURITY

**After completing this chapter, you will be able to:**

- Describe why security is important in Windows 2000
- Define auditing in Windows 2000
- Describe how auditing in Windows 2000 differs from that in Microsoft Windows NT 4
- Name the log file that contains all auditing entries
- Describe the three key pieces of information that auditing can provide
- Describe how auditing policies are integrated into Group Policy
- Know the order in which policies are applied on a Windows 2000 computer
- Know how to configure and implement auditing policies on a Windows 2000 system
- Describe available policy options available for files, folders, Active Directory objects, and printers
- Describe and define the purpose of security templates
- Describe and use the Security Configuration and Analysis tool

Few tasks are more important than making sure your Windows 2000 network environment is secure. Windows 2000 ships with many different tools that are designed to help you configure, implement, and support your security infrastructure, and we will look at the key tools in this chapter.

Security works at many different levels. You can't click on a single button to achieve a secure network. In fact, in order to ensure that invalid users do not access data on your network, you must form a comprehensive plan for how you will approach the issue, and then follow through with vigilance and enforcement.

Securing a network is a question of balance. The more secure your network needs to be, the more work you probably will create for yourself—it will take you longer to design your security plans, to implement your plans, and to maintain your policy. A network that is *too* secure might generate more support calls or prevent you from achieving the goal of making your network invisible to your users. On the other hand, a network that is not secure enough could create havoc.

Security is about preventing unwanted actions from occurring on your network. It includes preventing unauthorized access to resources or documents, validating users or groups if necessary, and making them accountable for the operations they perform. Security is a vital part of your initial network design, driving such factors as the creation of user accounts, groups, and Organizational Units (OU); delegation of authority; placement of domain controllers; replication strategies; and so on.

Fortunately, Microsoft has provided several tools to help you take control of your network. The flexibility of these tools means you can have a very secure network, or a less secure one. The balance is largely due to administrative overhead. The network should be as secure as you need it to be—but no more, because it will take time to monitor the network and maintain the policies you put in place.

When we think of security, we often think about two key areas: Who can access the network (user accounts), and what can a user do while on the network (resource management). In simple terms, does the user have a valid username and password? And, does the user have sufficient rights on the network to access the files and shares he or she needs? These concerns have not changed much from previous versions of Microsoft Windows NT, but the method by which these restrictions are achieved has changed. By leveraging the new feature set of Windows 2000, Microsoft has developed a scalable, manageable, and robust security infrastructure. With some careful design and implementation guidelines, and armed with a good understanding of how they work, you should be able to implement a policy that covers all areas of concern.

But, of course, security involves more than simply deciding what needs to be secure and then following through with assigning permissions. You also need to monitor your configuration. In fact, monitoring is a key consideration, and this area can increase both the cost and labor involved in making sure your network is secure. Security is a balance between convenience and administrative workload. The more secure you make your network, the more work you as an administrator will have to do up front, and also as you move forward.

The policies you put in place will need to be monitored and maintained. They should be reviewed periodically to make sure you are achieving the goals you set. This review will involve using familiar tools such as Event Viewer, and less familiar tools such as the Security Configuration and Analysis Console. Checking your security options should become one of your daily (or weekly) administrative tasks (along with maintenance chores such as checking the success or failure of backup operations).

Because Windows 2000 offers many tools and methods of securing a network, you need to be introduced to the range of tools and how they can be used. The security requirements for your organization will vary. Therefore, it is impossible for us to detail every option you will want to use. By introducing you to the features of each option, however, we can help you decide which tool to use, and how easy or difficult it will be for you to achieve the level of security you require.

## What Is Auditing?

As a system administrator, you will want to know what is going on in your network. But how can you do this when your network is dispersed within your organization, and probably across different countries? The answer is the built-in auditing function of Windows 2000.

Auditing has been available for quite some time in Microsoft Windows NT 4. However, because Windows 2000 has more features and different methods of maintaining user accounts and various other objects within Active Directory, you will find that the configuration interface (and the number of functions that can be audited) has changed. We will look at how you use the auditing functions; before we do, however, let's examine what can be audited, and what the repercussion of auditing can be.

**Auditing** is the ability to keep a record of certain events and activities. In fact, any activity that involves a Windows 2000 security object can be audited. These events are displayed in the Security Log of the local machine. Security Logs will be covered in more detail later in this chapter. For now, all you need to know is that you can view the Security Log in the Computer Management utility.

By default, the Security Log is empty, because by default Windows 2000 does not perform any auditing. This behavior does not mean that all the security mechanisms are not in place and working—it simply means that a log of these events is not being written. You can think of a log as a bank statement; it details everything you have asked it to track. By default, it tracks nothing.

It is a good idea to audit important events on your system—so why is the default *not* to audit? The problem is, auditing an event takes processing time, and a log can also consume quite a bit of CPU time and hard disk space. In fact, auditing every event is a good way to cripple a machine.

We need a sensible implementation of auditing. We will look at some of the events you might want to audit during this discussion. But first, let's consider the types of information you can expect to see in the Security Log.




You should remember reading about Event Viewer and the various logs it displays in Chapter 8. If not, then you might want to go back and look at that discussion before continuing. This chapter concentrates entirely on the Security Log, but many other useful logs available on domain controllers will also be of interest to you.

Three pieces of key information are recorded for audited events in the Security Log. These pieces of information are:

- The action that was being performed
- The user who performed the action
- The failure or success of the event and when it occurred

It's important to remember that these events are recorded at the location the events took place. So, let's say you have a share on a system, and access to this share has been limited to a small group of people. Someone from outside this group tries to access the share, and you have turned on auditing to capture this event. The event will be recorded at the server that is denying the access—in this case, the server where the share is located.

The dispersed nature of these log files means you must come up with a process for keeping track of them all. In this case, it might be a good idea to archive the log files, so the data in them is never lost. Then, you can peruse them at your leisure.


It is worth noting that not everyone can look at Security Logs. You need special permissions in order to read and configure them. The minimum permission you will need is the Manage Auditing And Security Log user right on the computer you want to access. In addition, the files for auditing must be stored on an NTFS partition. Although legitimate reasons can exist for storing data on FAT32 or even FAT partitions, it is generally better to overcome those restrictions and make the switch to NTFS as soon as possible.

Of course, it is entirely possible to read the log files of a remote computer from your own system. To do so, just follow these steps:

1. Choose Start | Programs | Administrative Tools | Computer Management to open the Computer Management console.
2. Click on System Tools and then click on Event Viewer to display the available log files in the right-hand panel. Notice the Computer Management (Local) entry at the top of the left-hand panel. The significant part is *Local* in parentheses—it tells you that you are currently looking at the log files for the local machine.
3. Right-click on Computer Management (Local) and select Connect To Another Computer to bring up the Select Computer dialog box. You can select another computer from this list, or type the name of the system you want to connect to in the Name text box.
4. You will be connected to the remote machine. Click on System Tools and Event Viewer to view the log files for the remote machine.

## Planning Your Audit Policy

You should consider several things before deciding on your auditing policy. First, what events do you really want to audit? The options are quite amazing, from every successful (or unsuccessful) attempt to use a printer, to the successful logon of every client. Auditing them all would generate a lot of data! So, you should audit only a subset of this data.

Second, you must decide which computers you will audit. It is unlikely that you will be concerned with every computer in your environment. For instance, is it really necessary to audit every event on each Windows 2000 Professional computer? Probably not. Identify those machines that you want to know about up front.

Two types of events can be audited: the success of an action and the failure of an action. In determining which events you are interested in, you should also decide whether you are interested in just the successful attempts that relate to the event, whether you are interested in the failures, or both.

Although this might not sound like a significant difference, it will dictate the types of information you can gain from the collected data. For instance, if you want to find out how many people are accessing a shared resource—perhaps a printer—then you will audit successful attempts. On the other hand, if you are more interested in security breaches (and attempts at breaches), then auditing failures would be more pertinent. When you audit logon attempts, this information can become even more important.


Auditing failed logons is a common usage. However, you'll be amazed how many of your users type the wrong password each morning. They'll even do it multiple times. Don't be surprised at this phenomenon—it is unavoidable.

You should review your audit logs (the Security Log in Event Viewer) regularly. If you do not look at them at the beginning of each day, then you may miss a trend that is developing on your network. Make the review of the log files part of your daily routine. Without review, the collected data has no benefit.

When you are thinking about events you want to audit, be careful not to be too indiscriminate. Many different events take place, and auditing too many of them can place an unnecessary load on your server. Also, because reviewing the logs should be part of your everyday routine, reviewing them will take a long time if you have audited many different parameters.

Generally speaking, successful attempts occur more frequently than failed events. Keep this in mind as you are determining what to audit. We're not saying you should not keep an eye on success events; but you should be clear about the reasons you are auditing an event. Will you really use the data for something? Don't collect data simply for the sake of doing it.



If you want to see trends over time, then you will have to archive the log files periodically. **Archiving** means making a copy of an event log for review at a later date. Many auditing options are available, such as overwriting events that are a certain number of days old, or overwriting after the log file reaches a certain size. If you use either of these options, then the records in the log are overwritten. This step prevents you from seeing a trend that might develop over a period of days, weeks, or months.


It is also a good idea to audit the events of the Everyone and Administrators group. By auditing the Everyone group, you can track the events associated with anyone who can access resources on your network. This audit is in contrast to tracking user groups, which may or may not include all users as members. Tracking the Administrators group allows you to track all events caused by administrators on your network. Doing so will enable you to see at a glance what your administrators have done.

Your environment may contain many servers, and you might wonder how you can configure each of them to audit certain events. In previous versions of Microsoft Windows NT, you configured these settings on a machine-by-machine basis. In the Windows 2000 world, Microsoft has incorporated these settings into Group Policy. In order to understand how these settings work, you should have a good understanding of Group Policy.

As you will see as you work your way through this chapter, many configuration options can be controlled from Group Policy. Actually, Group Policy lies at the heart of your auditing strategy. It will enable you to configure a group of settings in one place, and then have them applied to multiple machines in your organization.

## Local Policies and Domain Policies

We should make one last point before we dig into the specifics of what can be achieved with the security options of Windows 2000. Because policies and settings have been around for quite some time, it is useful to know how the old policies interact with the new, and what makes the current policies different than those that came before. What follows is a very brief recap of some of the finer points of Group Policy and how they relate to auditing in Windows 2000.

We have already stated that your security policies can be applied through Group Policy. This is significant, because it defines the level at which these policies can be assigned. If you recall from Chapter 10, these policies can be applied at three levels: the site, the domain, or the Organizational Unit. The acronym SDOU is worth remembering—it not only defines at what levels policies can be applied, but it also defines the precedence for multiple policies.

Other than applying policies through Group Policy, you can use two additional methods to set them at a computer. The first is called a **local policy**. As you might guess, such a policy is set at a single machine, and it affects only that one machine. Second, you might have older policies hanging around from your Windows NT 4 days. They can still be applied to Windows 2000 machines, although this practice is not recommended.

Why should you never use older style system policies on Windows 2000 machines? The answer is subtle, but very significant. In the older style policies, changes were made to the Registry of the clients, meaning that a physical change was made to the Registry. The value for a key was changed from one value to another value. This feature was known as **tattooing**.

Tattooing actually gave you less control over what was happening on a machine. With the newer policies, if a policy is not applied for some reason, then the original Registry setting still exists and takes its place.


Group Policy is better than the old style system policies for a few other good reasons. For one thing, NT 4 system policies are contained in a single file, NTCONFIG.POL. This file must take into account all the different policies you want to apply. It can become quite huge. Second, the sheer number of policy settings that can be applied now has increased substantially.

Local policies are stored on the local machine. Group policies are stored in both the Active Directory and on each domain controller. They are replicated from one domain controller to another by the File Replication Service. These details are covered in Chapter 10.

You may be thinking that multiple policies can be applied, and it might be tricky to figure out which one will be applied and which one won't. Let's clear up this question before we go any further. The following list shows each policy that exists. They are given in descending order, which means the policy at the top of the list is applied first. If the next policy includes a conflicting setting, then the next policy wins:

- System policies (Windows NT 4)
- Local policies
- Site policies
- Domain policies
- OU policies

One of the simplest examples is the wallpaper on a system. Let's say a different default wallpaper is assigned in each policy. This wallpaper has the name of the policy written on it. First, the wallpaper would read *system policies*; then it would change to *local policies*, and so on. By the time everything had been calculated, the wallpaper would read *OU policies*, because these policies always end up winning when there is a conflict.

You may wonder how you can tell which policies have been assigned to a computer. Later in this chapter, we will look at a tool called the Security Configuration and Analysis Console, which handles this task.

We hope this brief recap will help you troubleshoot any issues you might have when setting auditing policy through Group Policy in Windows 2000. Now, let's look at how you configure auditing in Windows 2000 through Group Policy.



## Configuring Group Policy

Configuring auditing is a two-step process. First, you must enable auditing, which means objects can be audited on your system. Doing so does not turn on auditing, however, because far too many auditing events exist. Turning them all on would have a bad effect on your computer. Instead, a second step allows you to go in and select the specific objects and events about which you want to gather auditing information.

Because these security options are configured through Group Policy, it should come as no surprise to find that you will need to access the Group Policy snap-in to make these changes. Nine event categories can be audited from within Windows 2000. These categories can have many different events assigned to them; so once you have enabled a

category, you must then configure the specific events you want to capture. Figure 15-1 shows the categories as they appear in the Group Policy console.

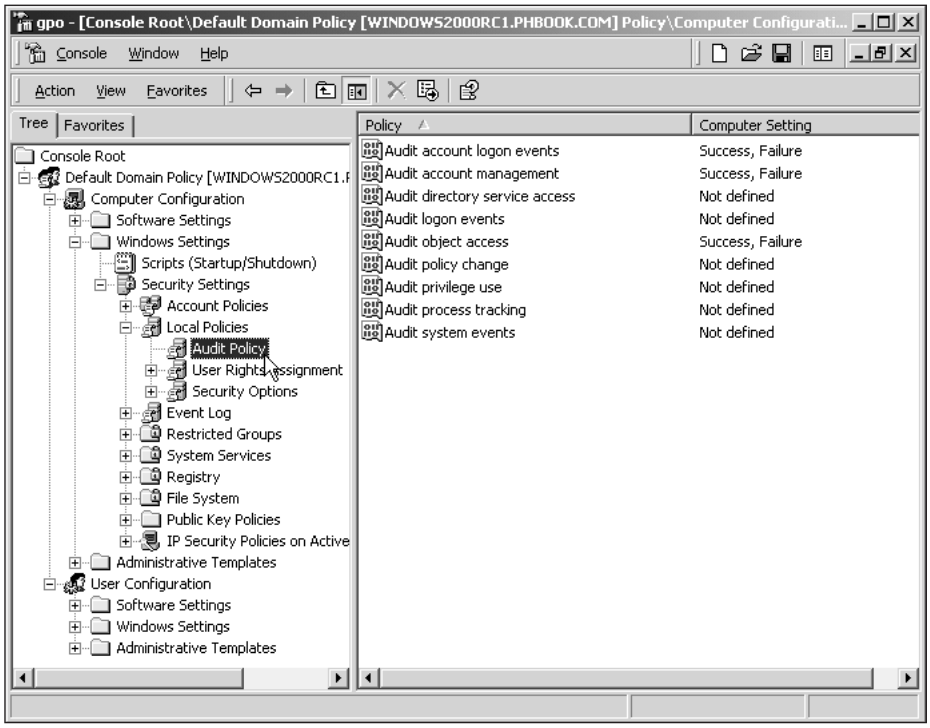


**Figure 15-1** The types of events that can be audited in Windows 2000

Table 15-1 gives a brief explanation of what each category covers. We will look at more specific events associated with some of these categories later in this chapter.

**Table 15-1** Definitions for auditing categories

| Category Name | Definition |
|---|---|
| Account Logon Events | Records the event when a domain controller receives a request to validate a user account. |
| Account Management | Audits changes made by administrators to user accounts or groups. These changes include renaming, creating, or deleting accounts. This category will also record an entry when password changes take place. |
| Directory Service Access | Records an event if a user accesses an object in Active Directory. This setting is configured on a per-object basis. |

**Table 15-1** Definitions for auditing categories (continued)

| Category Name | Definition |
|---|---|
| Logon Events | Audits specific users' logging on and logging off a system. This event also allows you to audit users who are making (or canceling) a connection to a server. |
| Object Access | Similar to Directory Service Access. More specifically, however, this setting allows you to audit access to files, folders, or printers. It is set at a per-resource level, so you will need to configure it for each share, file, or printer. |
| Policy Change | Records events relating to changes in auditing policies, user rights, or user security options. |
| Privilege Use | Records an event when users exercise one of the rights they have been assigned. These events can quickly fill a Security Log. This setting does not include events for logging on or off, because they are audited in another category. |
| Process Tracking | Tracks actions performed by a program on the server. You might use this option to track the events of a third-party application, although it is only of specialized interest. |
| System Events | Tracks some significant system events, such as the restarting of a Windows 2000 system. This setting also records events that are specific to the Security Log, such as the log's being full, or events being deleted from the log. |

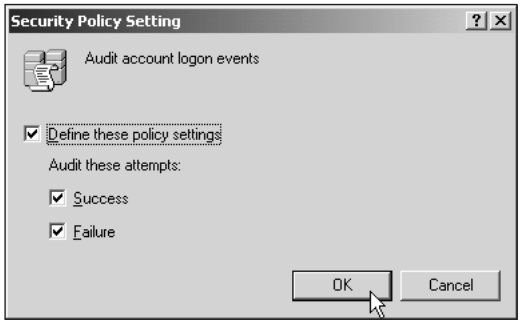


**Figure 15-2** The Security Policy Setting dialog box

Before you can go down to the object level and allow events to be audited, you must first turn on auditing for that category. The Security Policy Setting dialog box is shown in Figure 15-2. As you can see, you can configure relatively few options at this level: auditing of successes, failures, or both. Once you have configured this dialog box, you can choose some events to be audited.


Policy changes made in Group Policy can take time to propagate throughout the domain. If you make a change in Group Policy, then you have three choices: You can wait for the change to propagate, restart the computer (causing the Group Policy objects to be read), or force the new settings to be applied. You do this by using the command-line utility secedit. Use the following syntax:

```
secedit /refreshpolicy machine_policy
```

## Auditing Files and Folders

Because it is beyond the scope of this book to cover every auditing event that you might want to record, we have chosen to discuss file and folder access. These items can be audited only if the Object Access option has been enabled with either Success or Failure.

As you will see, when you get down to the object level, many different events can be audited. For instance, at the file and folder level there are no fewer than 13 specific events. In order to explain the levels at which auditing can be performed, we will list each of the entries that can be enabled for the auditing of file and folder usage. Figure 15-3 shows these options.

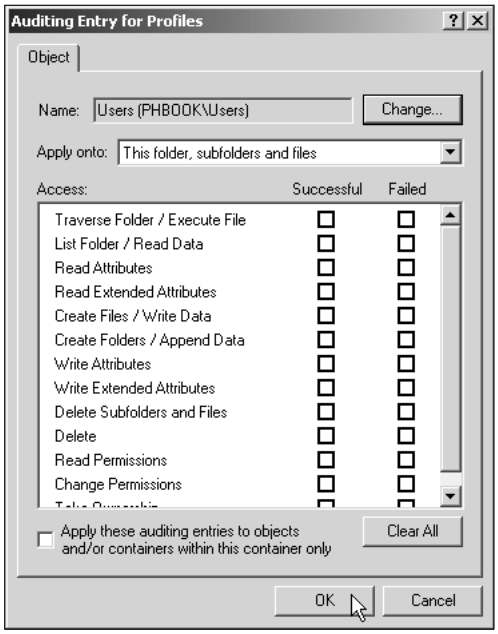


**Figure 15-3** The Auditing Entry dialog box

Although we have said this more than once already, it is worth restating that it is not a good idea to turn on all the options. Try to be discerning and work out what information will be useful for you to know.

Table 15-2 explains what the file- and folder-level events mean. You have a fine level of granularity you can use for auditing files and folders. You can also choose whether the settings you configure should apply only to the current files and folders, or whether the folders and files stored in subfolders should inherit the settings. This choice is important because you can easily create too many entries in the Security Log by mistake. Note that by default, settings made in a folder are inherited by all subfolders.

**Table 15-2** Auditing categories for files and folders

| Category Name | Definition |
|---|---|
| Traverse Folder/Execute File | Records an event if a user moves through folders to gain access to a folder or share. Also records an event when a program runs. |
| List Folder/Read Data | Records an event when a user views the folder names or file names. Also records an event when a file is read. |
| Read Attributes | Records an event when a user displays the attributes of a file or folder. |
| Read Extended Attributes | Records an event when a user displays the extended attributes of a file or folder. |
| Create Files/Write Data | Records an event when a file is created in a folder, or when the data in a file is changed. |
| Create Folders/Append Data | Records an event when a folder is created in a folder, or when a file has data appended to it (without overwriting the file). |
| Write Attributes | Records an event when an attribute on a file or folder changes. |
| Write Extended Attributes | Records an event when an extended attribute on a file or folder changes. |
| Delete Subfolders And Files | Records an event when a file or folder *within a folder* is deleted. |
| Delete | Records an event when a file or folder is deleted. |
| Read Permissions | Records an event when a user views the permissions or owner of a file or folder. |
| Change Permissions | Records an event when permissions of a file or folder are changed. |
| Take Ownership | Records an event when someone takes ownership of a file or folder. |

Some of these options might have limited value to you—so many auditing options exist that it can be difficult to choose between them. Along with files and folders, you should learn about auditing two other areas. First we will look at Active Directory objects, and then we will look at printers. The basic principles are the same, but the events that can be audited change.

## Auditing Active Directory Objects

No fundamental differences exist between configuring auditing for Active Directory objects and configuring auditing for files and folders. In order to audit Active Directory objects, you must have enabled auditing for the Directory Services Access object. Once you have done this, you can configure the specific events you want to audit.

When auditing Active Directory objects, you can configure auditing for specific objects such as users, computers, groups, or OUs. These objects cover a broad sweep and can generate a lot of data. We will look at configuring some of them later in the chapter. In the meantime, let's examine the types of events that you can audit when working with Active Directory objects. Because there are 43 options, Table 15-3 lists only those that are most commonly used.

**Table 15-3** Auditing categories for Active Directory objects

| Category Name | Definition |
|---|---|
| Full Control | Records an event when any type of access is made to the object |
| List Contents | Records the viewing of objects stored within the audited object |
| Read All Properties | Records viewing of any attribute |
| Write All Properties | Records the change of any attribute |
| Create All Child Objects | Records the creation of any object within an audited object |
| Delete All Child Objects | Records the deletion of any object within an audited object |
| Read Permissions | Records the viewing of the permissions for an audited object |
| Modify Permissions | Records the change of the permissions for an audited object |
| Modify Owner | Records an event when a user takes ownership of an audited object |
| Create Printer Objects | Records the creation of a Printer object within an audited object |
| Delete Printer Objects | Records the deletion of a Printer object within an audited object |
| Create User Objects | Records the creation of a User object within an audited object |
| Delete User Objects | Records the deletion of a User object within an audited object |
| Create Shared Folder Objects | Records the creation of a shared folder within an audited object |
| Delete Shared Folder Objects | Records the deletion of a shared folder within an audited object |

You can choose many additional options when auditing Active Directory objects. Some of them are good for security options, whereas others can simply act as a record of what is occurring on your network—such as administrators doing their jobs.

It is also worth noting that these settings can also be configured for inheritance. By default, all settings are inherited by child objects.

## Auditing Printers

You might also want to audit access to printers. For instance, you may want to audit access to printers that are sensitive—such as those in secure areas of your building, or those that belong to directors or managers.

Once again, the general guidelines are much the same as you have seen before. In order to audit printers, you must enable auditing for object access. Once you have done this, you can configure the events you want to record. These events are defined in Table 15-4.

**Table 15-4** Auditing categories for printers

| Category Name | Definition |
|---|---|
| Print | Records the printing of a file |
| Manage Printers | Records changes made to the printer settings, such as pausing or sharing a printer |
| Manage Documents | Records changes made to job settings, such as pausing, restarting, moving, or deleting documents |
| Read Permissions | Records the viewing of printer permissions |
| Change Permissions | Records changes made to printer permissions |
| Take Ownership | Records an event when a user takes ownership of the printer |



## Tips for Auditing

You can audit so many things, you could be forgiven for getting somewhat confused about best practices. With that in mind, we will discuss some things to consider when deciding upon your auditing policy.

If you are worried about hackers or other unauthorized users getting into your network, then it is a good idea to audit failed logons. These logons will inform you when users try to log on with bad passwords. Keep in mind that hackers have programs that can repetitively try different passwords on a user account. Combined with lockout policy on your Windows 2000 network, this event can give very useful information.

If you suspect that someone is using an account without permission, then it can be useful to audit successful logon attempts. In this case, you will look for logins that happen after hours, or when the owner of the account is absent.

If you suspect users are trying to access files or folders to which they do not have permission, then you should audit failure of object access. As detailed in the previous paragraph, if you think access is being gained through a legitimate account, then you might want to audit successful attempts, also.

## Security Templates

Until now, we have looked at some of the options that can be configured for auditing. As you have seen, these options are very powerful, and there are many to choose from. Setting up each option can be time consuming, however, and doing so requires an intimate knowledge of all the available options. Wouldn't it be nice if Microsoft provided some default settings we could use?

Well, Microsoft did just that! These settings are called **security templates**. Security templates are merely collections of settings that alter auditing or security settings. These templates can then be imported into a Group Policy Object (GPO) and applied to sites, domains, or OUs.

Security templates are actually text files with an .inf file extension. Because they are text files, it is possible to cut and paste sections between templates, or to edit the files directly (although doing so is not recommended). Not only can these files be imported into GPOs, they can also be exported. Exporting is useful when you need to back up a security configuration on a machine. If you export the security settings made in the local policy on a machine, you can then import the policy into similarly configured machines, or use it to restore a machine's lost security settings.

Microsoft has provided several preconfigured template files. You can use these files as they are, or edit them to make any adjustments you see fit. In the following section, we will discuss some of these templates and how you can use them.

### Preconfigured Security Templates

The preconfigured templates that ship with Windows 2000 are based around computer roles and scenarios. These combinations cover such instances ranging from standalone servers operating in a low-security environment to domain controllers in a high-security environment.

Before you use these templates, it is important that you make a thorough analysis and evaluation of their effectiveness. You should learn the details of what each contains, and then test the templates in a lab. Failure to do so can cause problems on a network due to unexpected behavior.

It probably comes as no surprise to find out that Microsoft ships many templates with Windows 2000. As you can see in Figure 15-4, 13 templates are predefined. You can find them in the <*systemroot*>\Security\Templates folder. Let's take a moment to define briefly what each is intended to do. Don't forget, we mentioned earlier that these templates were designed based on roles and scenarios. Table 15-5 defines the role for which each template was designed.

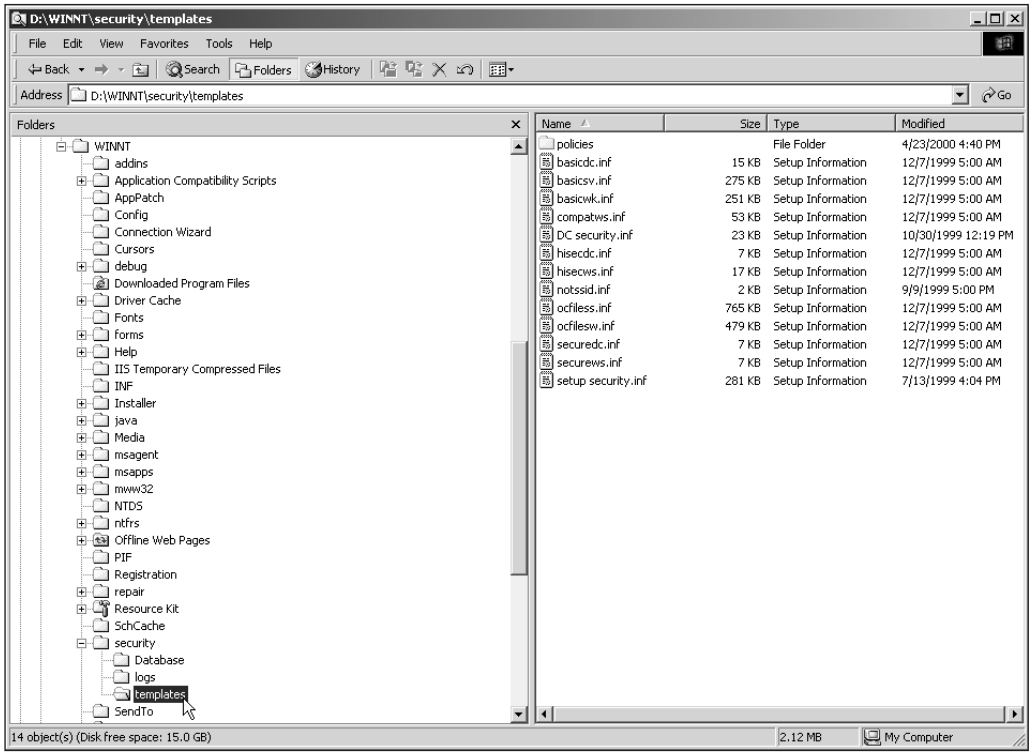


**Figure 15-4** Security templates shipped with Windows 2000

**Table 15-5** Defining security templates

| Template Name | Role Definition |
|---|---|
| basicdc.inf | Default security settings for a domain controller |
| basicsv.inf | Default security settings for a standalone (or member) server |
| basicwk.inf | Default security settings for a Windows 2000 Professional system |
| compatws.inf | Security settings that make the Professional server backward compatible with Microsoft Windows NT 4 |
| DC security.inf | Default settings (updated) for domain controllers |
| hisecdc.inf | High-security settings for a domain controller |
| hisecws.inf | High-security settings for a Windows 2000 Professional system |
| notssid.inf | Removes the Terminal Server SID assigned to a Windows 2000 Server |
| ocfiless.inf | Optional component file settings on servers |
| ocfilesw.inf | Optional component file settings on Windows 2000 Professional |
| securedc.inf | Secure domain controller settings |
| securews.inf | Secure Windows 2000 Professional settings |
| setup security.inf | Default settings applied after installation (installation defaults) |

With the exception of three of the above templates—ocfiless.inf, ocfilesw.inf, and notssid.inf—you may have noticed that the others share some naming similarities. These names indicate the level of security (or scenario) that each template has been designed to achieve. It is useful to define these four scenarios for your future reference:

- *basic*—Any template with the term **basic** in its name was designed to return a system to the default settings if they have been changed. Such a template acts as a default starting point. It is worth noting that these templates do not alter user rights on a system; applications might have altered these rights, and undoing them would cause problems. If a system has a problem that you feel is due to a change that has been made to security settings, then use the basic templates.
- *compat*—Templates with **compat** in their names are actually "compatible" templates. Windows 2000 systems have some settings that are different from those you might have seen in previous versions. For instance, by default in Windows 2000, users logging in to a Windows 2000 Professional system are Power Users on that system. These security templates prevent this type of behavior—in this example, by removing all users from the Power Users group.
- *secure*—Any template with **secure** in its name is a recommended template for a system. These templates enforce changes to all areas except files, folders, and Registry keys. They do not make changes to these areas because, by default, the areas are secured.

- *hisec*—Templates with **hisec** in their names are highly secure. These templates are aimed at network communications. They configure security settings for both network traffic and protocols. These settings will prevent a Windows 2000 system from communicating with any down-level clients, including Windows 9*x* and Microsoft Windows NT 4 systems.

## Viewing Security Templates Configurations

All this talk about each of the available templates is pretty interesting, but let's look at what they contain. As you can imagine, examining every setting in each of these templates is daunting. So instead, we will walk you through the process you can use to view and edit these templates.

In the following example, you will create a new Microsoft Management Console (MMC) containing the Security Template snap-in. You will use this snap-in extensively when configuring the security templates. Don't forget, the MMC is very flexible. In this example you will end up with a new MMC with this single snap-in included, but it would be very easy to add the snap-in to any other console you use regularly. Follow these steps:

1. Open a blank MMC. To do so, choose Start|Run and type "MMC". Press Enter. The MMC will open with an empty Console Root.
2. Click on the Console menu and select Add/Remove Snap-In to open the Add/Remove Snap-In dialog box. This dialog box lists the snap-ins that are currently being displayed. This is a new MMC, so the entries are blank.
3. Click on Add to display the Add Standalone Snap-In dialog box. This dialog box displays all the available snap-ins on your system. Scroll down the list until you find the Security Templates snap-in. Click on it to select it. Click on Add. You should see the snap-in displayed in the Add/Remove Snap-In dialog box.
4. Click on Close to close the Add Standalone Snap-In dialog box. Click on OK to exit the Add/Remove Snap-In dialog box. Doing so returns you to the MMC. It should now resemble the MMC shown in Figure 15-5.
5. Double-click on Security Templates in the left-hand panel to display the path to the security template files on your system. Double-click on the path to see a list of all of the templates. Double-click on the first entry—basicdc—to see the group of settings that have been used in this template. By clicking on each of these groups, you can see the specific settings that have been made, as shown in Figure 15-6.


**Figure 15-5** An MMC containing the Security Templates snap-in

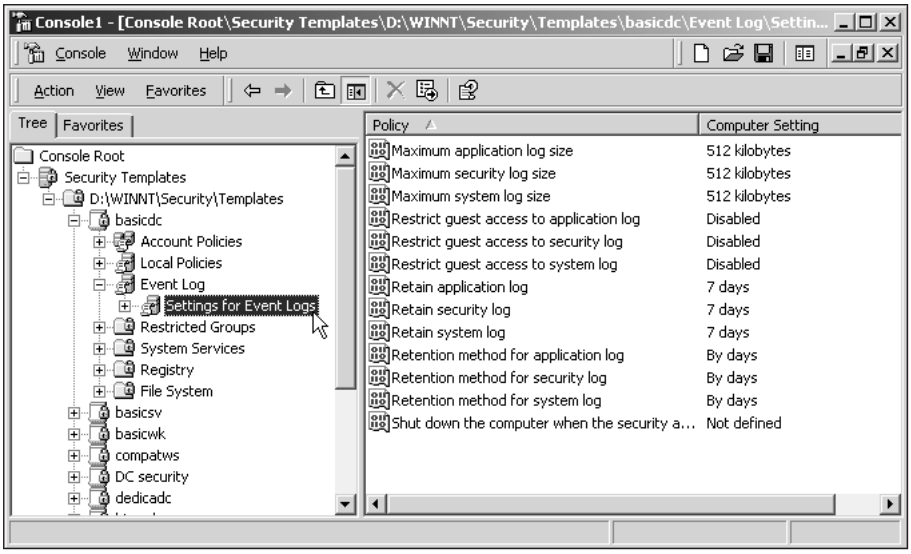


**Figure 15-6** The configured settings for the basicdc security template

6. To save this MMC for later use, click on the Console menu and select Save As. Type the name you want to use for the new MMC. By default, the new MMC files are stored in the Administrative Tools folder for the currently logged-on user. As a result, your new console will show up on the Start | Administrative Tools menu. Type "Security Templates" and click on OK.

It is possible to edit the templates that currently exist, or to create entirely new templates from within the Security Templates Console. To do so, simply right-click on the path name in the left-hand side of the console and choose New Console. You will be prompted for a name and description. Once this step is done, an INF file is created to contain your template settings, and an entry is displayed in the Security Templates Console.

## Using Security Templates with GPOs

The final piece of this puzzle is using the security templates with Group Policy. In order to apply one of the templates to a GPO, you will have to import the settings into local policies or nonlocal GPOs. Because the settings are preconfigured, configuring groups of computers or users is very easy. Importing the template settings into a GPO means that anyone who is a member of the GPO will be affected by the settings.

In the following example, we will use the Active Directory Users and Computers snap-in to apply a security template to a GPO. In the example, we have already created a new GPO for this purpose. Be careful when performing this example on a live system—you could inadvertently lock down (or undo) security settings that your administrators want in place. Follow these steps:

1. To open the Active Directory Users and Computers Console, choose Start|Programs|Administrative Tools and select Active Directory Users And Computers.
2. If you are using a production system, you may want to create a test OU for this example. To do so, click on your domain name and select New|Organizational Unit. You will be prompted for a name; enter "Security test" and click on OK. The new OU will be displayed in the left-hand panel.
3. To import one of the security templates so it is applied to this OU (and to any members of this OU), right-click on the new OU and select Properties from the menu. Select the Group Policy tab, shown in Figure 15-7.
4. To create a new GPO, click on the New button. An entry is shown in the dialog box. The default name for new GPOs is New Group Policy Object. Change this name to Security Test by typing "Security Test" and pressing Enter.
5. To import the settings, click on the policy you just created and select Edit to bring up the Group Policy Console. Double-click on Computer Configuration and then double-click on Windows Settings to display the screen shown in Figure 15-8.

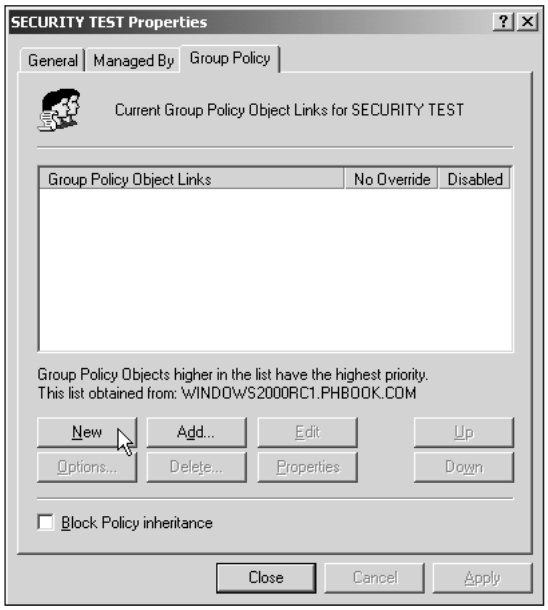


**Figure 15-7** The Group Policy tab

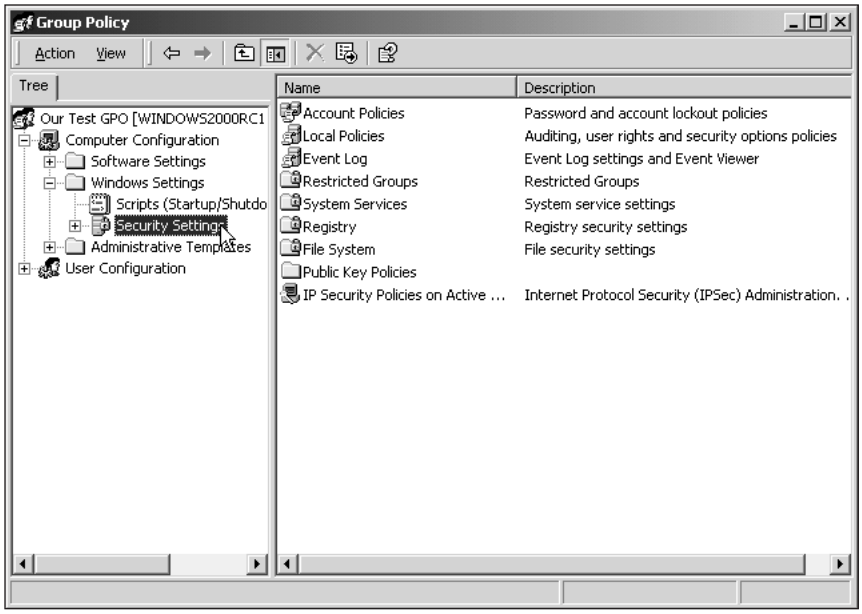


**Figure 15-8** The Group Policy Console

6. To import your template, right-click on Security Settings and choose Import Policy. (Note that the Export List option exports the current settings to an INF file.) Doing so opens the Import Policy From dialog box, which lists all the available INF files. For the purposes of this example, you will simply import the basicdc.inf. Select it and click on OK.

Security templates are a key part of your enterprise's security policy. You can create a set of configurations in one place and then reuse them throughout your organization. Because you do so via Group Policy, you can target sites, domains, and OUs with ease. This ability enables you to apply the settings to many different computers at one time.

## THE SECURITY CONFIGURATION AND ANALYSIS TOOL

The security settings on a single computer can be quite difficult to track. In fact, with Windows 2000, this difficulty can be accentuated because you can set so many additional options.

Realizing this potential problem, Microsoft came up with an MMC console snap-in called the Security Configuration and Analysis tool. This tool has several different uses: It can help you define the settings suitable for a workstation or server, and it allows you to analyze the effects of applying security templates to a system.

This tool is shown in Figure 15-9. As you can see, the MMC interface is immediately recognizable. You will be using this tool later in this chapter.

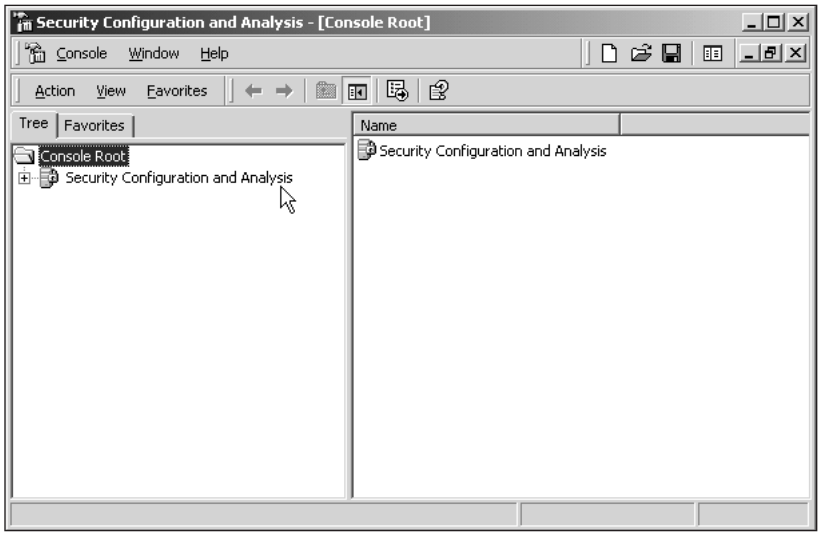


**Figure 15-9** The Security Configuration and Analysis tool

The Security Configuration and Analysis tool works by creating a database on the local workstation or server. This is one of the tool's drawbacks—because the database is stored locally, you must be at the machine to make it work. In some cases, this requirement might prevent you from using this tool. In networks where all systems are part of a domain, you can use the security templates applied at the GPO level to configure workstations, because the Security Configuration and Analysis tool is impractical.

Once you have created a local database, you can import security templates and have them applied to the workstation. The tool includes options to export and combine multiple templates to create a complete security configuration. Because these templates can be added one at a time, you can see the effects of layering one security template upon another. Where a conflict exists between templates being applied, the last one applied takes precedence. As they are imported, the security settings are applied to the system.

The analysis options of the Security Configuration and Analysis tool allow administrators to view the current settings on a system. Security settings are dynamic, because different users and applications require different levels of security. It is possible for a properly configured system to become noncompliant. This tool allows you to analyze the current settings and see which settings have changed.

Performing an analysis is an important part of your security plan. It is easy to overlook systems that are not part of the domain. Without the occasional review, you will not know what affect routine work is having on your systems. Although it can be difficult to visit every workstation, you should at least take representative samples and analyze them. A lab environment can be used—but you must make sure the lab computers closely resemble those in use on desks around your enterprise.

If you find a discrepancy between the settings on the current system and a security template, then you have several options. You can either accept the changes that the security template is about to apply, or you can accept the current settings and leave them alone. You can also arbitrarily return the system to the state defined by the template. Doing so will overwrite any settings that differ from those in the security template. This choice is useful if a system is not compliant with the security standard you have set for your enterprise.

Alternatively, you can change the settings for a system by importing another template. As you saw earlier in this chapter, many templates exist. If the role of a system changes—perhaps a standard server is being installed as a domain controller—you can easily use this tool to apply a new template.

Once the system database is properly configured and all conflicting security settings are resolved, you can apply the settings to the system. Note that this step is not performed until you specifically want it to be. The settings and conflicts displayed within the tool are simply those generated within the database. Changes made to the settings are database entries—you can decide either to apply them to the system or to ignore them.

## CHAPTER SUMMARY

- In this chapter, we looked at some of the options that can help you ensure that your network and systems are secure. We started our discussion by examining auditing. The auditing options in Windows 2000 allow you to trace events in your enterprise from a central location. This task is an essential part of system administration.
- You learned that events and activities are recorded in the Security Logs of the machines at which they occur. You can view the log using the Computer Management tool. Auditing is turned off by default, because it can put quite a strain on the server on which it is configured by eating both CPU time and disk space.
- You should review the Security Logs on your systems on a regular basis. No amount of auditing will secure your systems if you are not paying attention. It is a good idea to review the logs at the start of each day.
- Microsoft has provided an easy way to configure servers without having to visit each one. Auditing options can be applied through Group Policy.
- Several types of policy can be applied to a system, including local policies, site policies, domain policies, and Organizational Unit policies. Additionally, Group Policy can be applied at several different levels: site, domain, or OU. These levels are known by the acronym SDOU. The old-style Microsoft Windows NT 4 policies can still be applied, but it is a good idea to make an immediate switch to the newer Windows 2000 policy types.
- We then looked at the different categories of events and activities that can be configured on a system. You can choose from many different categories, and you should choose only those that are important to you.
- We saw that the file and folder level is one of the most common areas for auditing. Auditing at this level allows you to view many different events, such as the reading of a file, or the fact that a specific user has accessed a share.
- We also examined the options available when auditing access to Active Directory objects. Doing so allows the system administrator to track both the creation and deletion of objects, or the exercising of other security permissions.
- You may also want to audit printers in the enterprise. Printers are a valuable resource; they also represent an area of possible concern for security reasons. We saw that it is possible to record several types of events, including users who change permissions on printers or who change job settings.

- You learned that it is important to configure security settings at each system. You can do so through preconfigured security templates. These templates are provided by Microsoft. They can be used as is, or you can configure them to better suit your environment. We saw that templates are in place for standalone servers, domain controllers, and Windows 2000 Professional systems. Templates allow for three levels of security: normal, high security, and secure.
- These templates can be imported into GPOs, and are then applied to objects that are members of the GPO. This process allows for the widespread application of security settings in the enterprise—preventing you from having to visit each system. It also lets you make changes to security settings in one place and have them applied globally.
- Finally, we looked at the Security Configuration and Analysis tool. This tool allows you to view the security settings that are currently being applied to a machine so the settings can be compared to a desired state. It then displays the discrepancies. You can make necessary changes to the security settings and apply them to the system.
- The Security Configuration and Analysis tool is of limited use for systems that are part of a domain, because the tool requires that you have physical access to the system. However, it is useful for standalone systems.